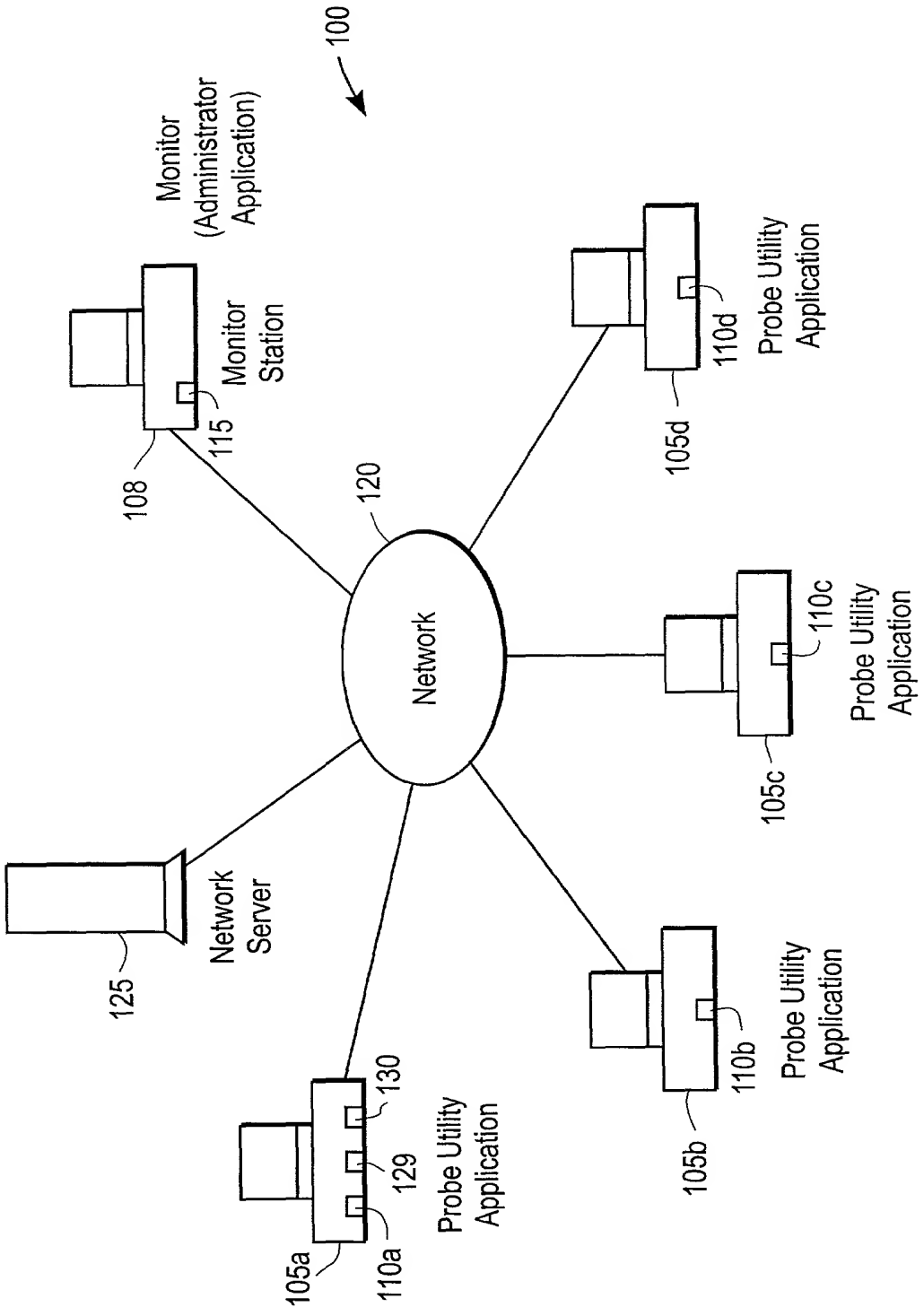

100
Monitor (Administrator Application)
Monitor Station
115
108
120
Network
Network Server
125
105a
110a
129
130
Probe Utility Application
105b
110b
Probe Utility Application
105c
110c
Probe Utility Application
105d
110d
Probe Utility Application

FIG. 1

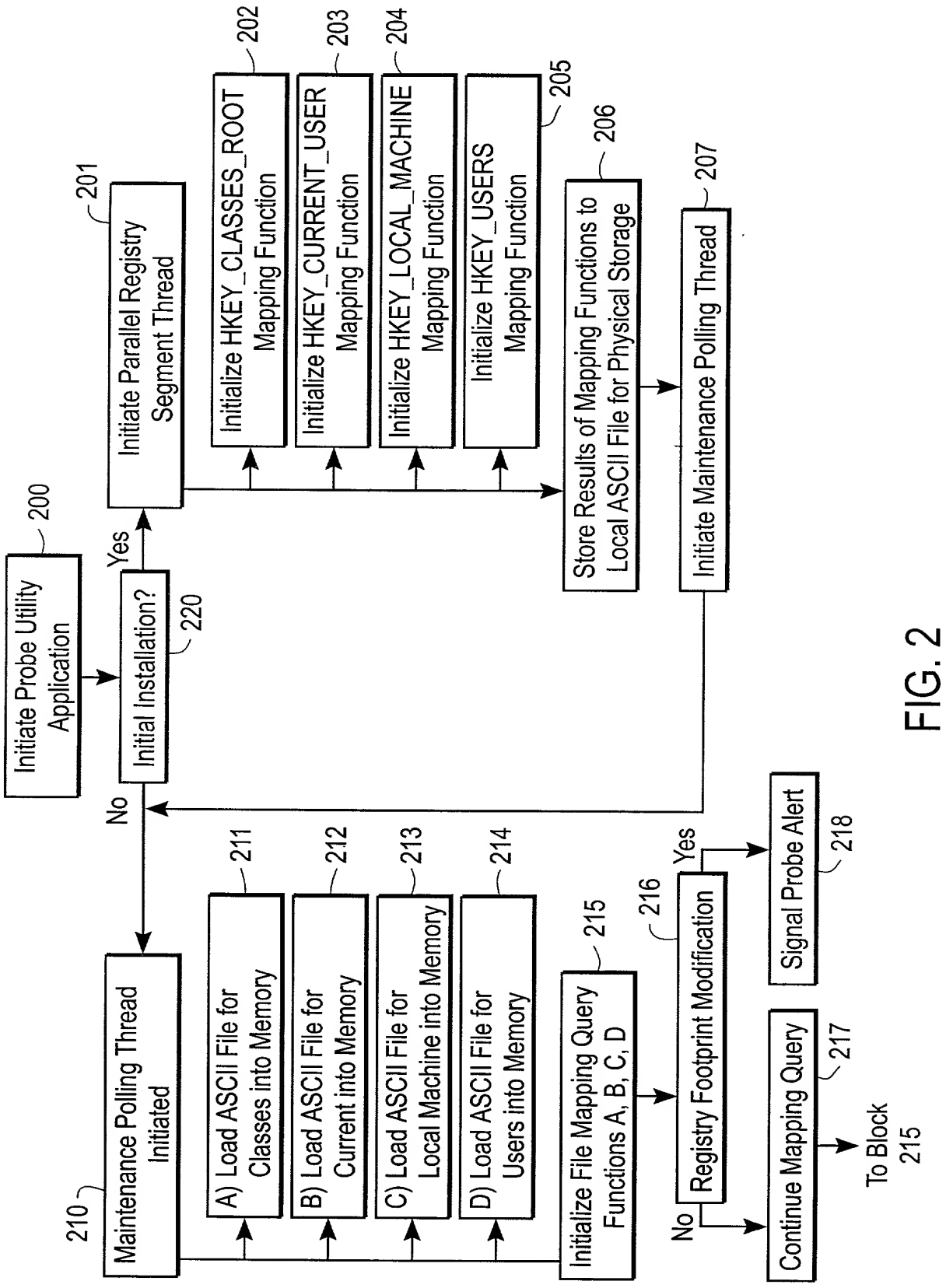

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Parallel Registry Segment Thread
201
Initialize HKEY_CLASSES_ROOT Mapping Function
202
Initialize HKEY_CURRENT_USER Mapping Function
203
Initialize HKEY_LOCAL_MACHINE Mapping Function
204
Initialize HKEY_USERS Mapping Function
205
Store Results of Mapping Functions to Local ASCII File for Physical Storage
206
Initiate Maintenance Polling Thread
207
Maintenance Polling Thread Initiated
210
A) Load ASCII File for Classes into Memory
211
B) Load ASCII File for Current into Memory
212
C) Load ASCII File for Local Machine into Memory
213
D) Load ASCII File for Users into Memory
214
Initialize File Mapping Query Functions A, B, C, D
215
Registry Footprint Modification
216
Yes
No
Signal Probe Alert
218
Continue Mapping Query
217
To Block 215

FIG. 2

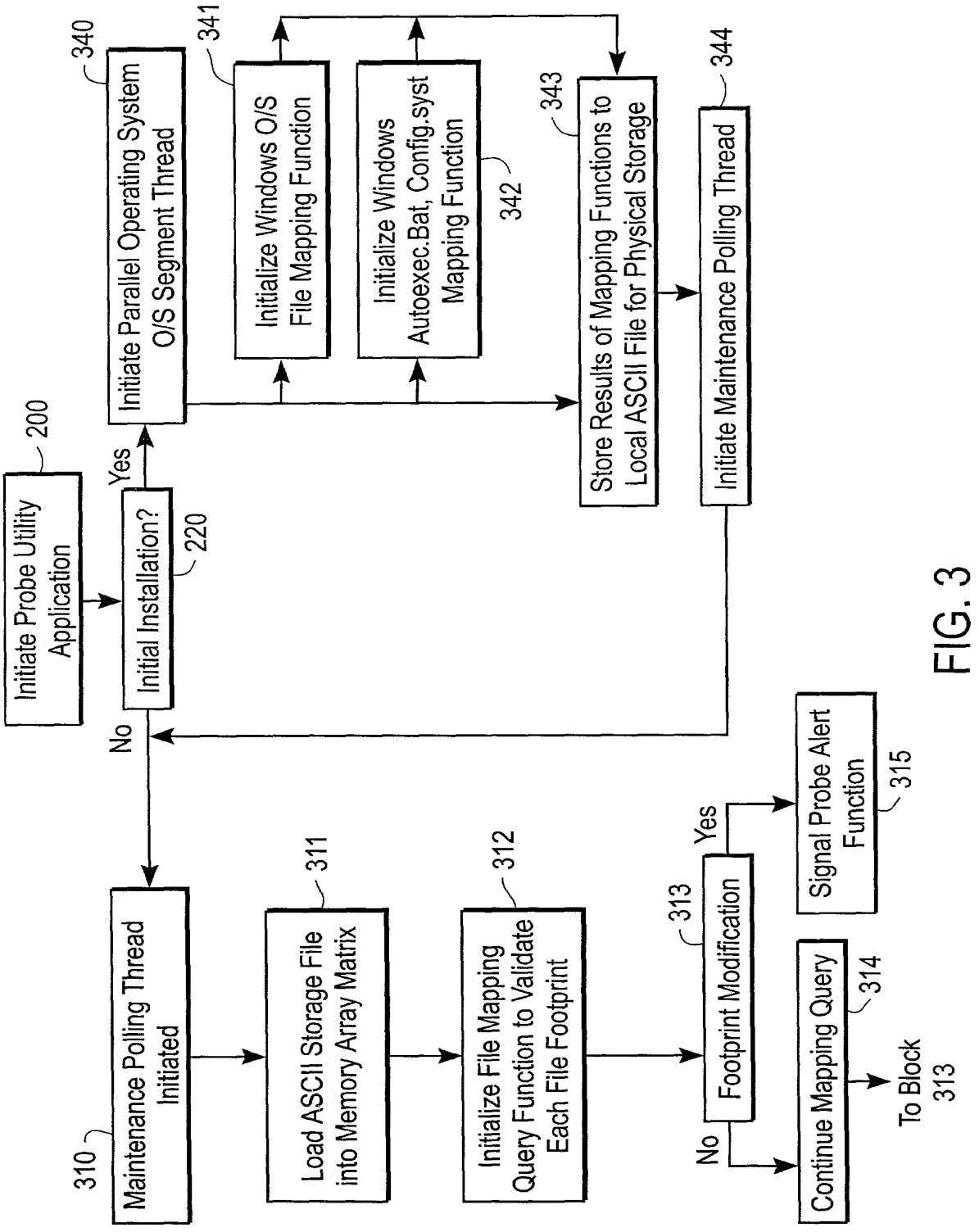

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Parallel Operating System O/S Segment Thread
340
Initialize Windows O/S File Mapping Function
341
Initialize Windows Autoexec.Bat, Config.syst Mapping Function
342
Store Results of Mapping Functions to Local ASCII File for Physical Storage
343
Initiate Maintenance Polling Thread
344
Maintenance Polling Thread Initiated
310
Load ASCII Storage File into Memory Array Matrix
311
Initialize File Mapping Query Function to Validate Each File Footprint
312
Footprint Modification
313
Yes
No
Signal Probe Alert Function
315
Continue Mapping Query
314
To Block 313

FIG. 3

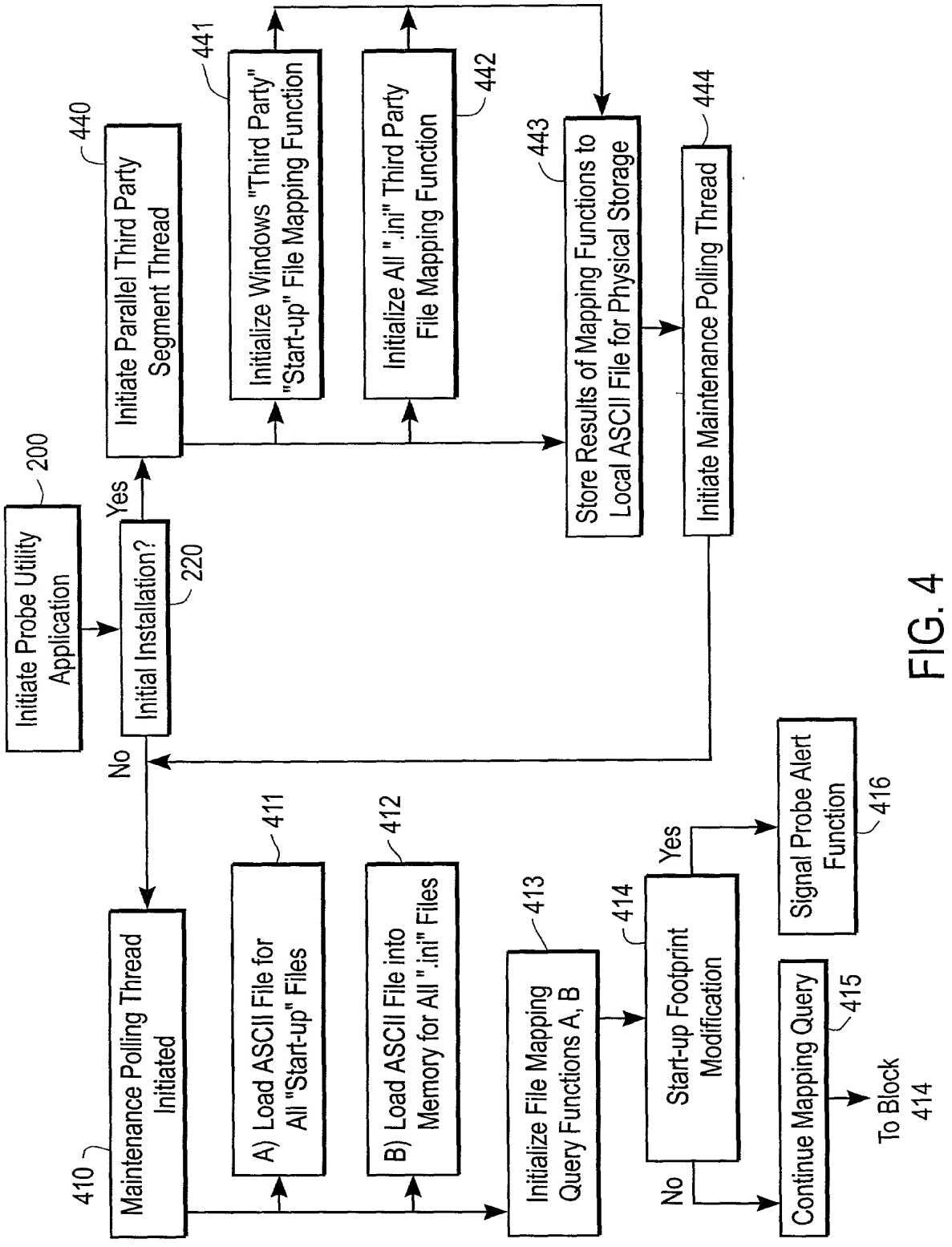

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Parallel Third Party Segment Thread
440
Initialize Windows "Third Party" "Start-up" File Mapping Function
441
Initialize All ".ini" Third Party File Mapping Function
442
Store Results of Mapping Functions to Local ASCII File for Physical Storage
443
Initiate Maintenance Polling Thread
444
Maintenance Polling Thread Initiated
410
A) Load ASCII File for All "Start-up" Files
411
B) Load ASCII File into Memory for All ".ini" Files
412
Initialize File Mapping Query Functions A, B
413
Start-up Footprint Modification
414
Yes
No
Signal Probe Alert Function
416
Continue Mapping Query
415
To Block 414

FIG. 4

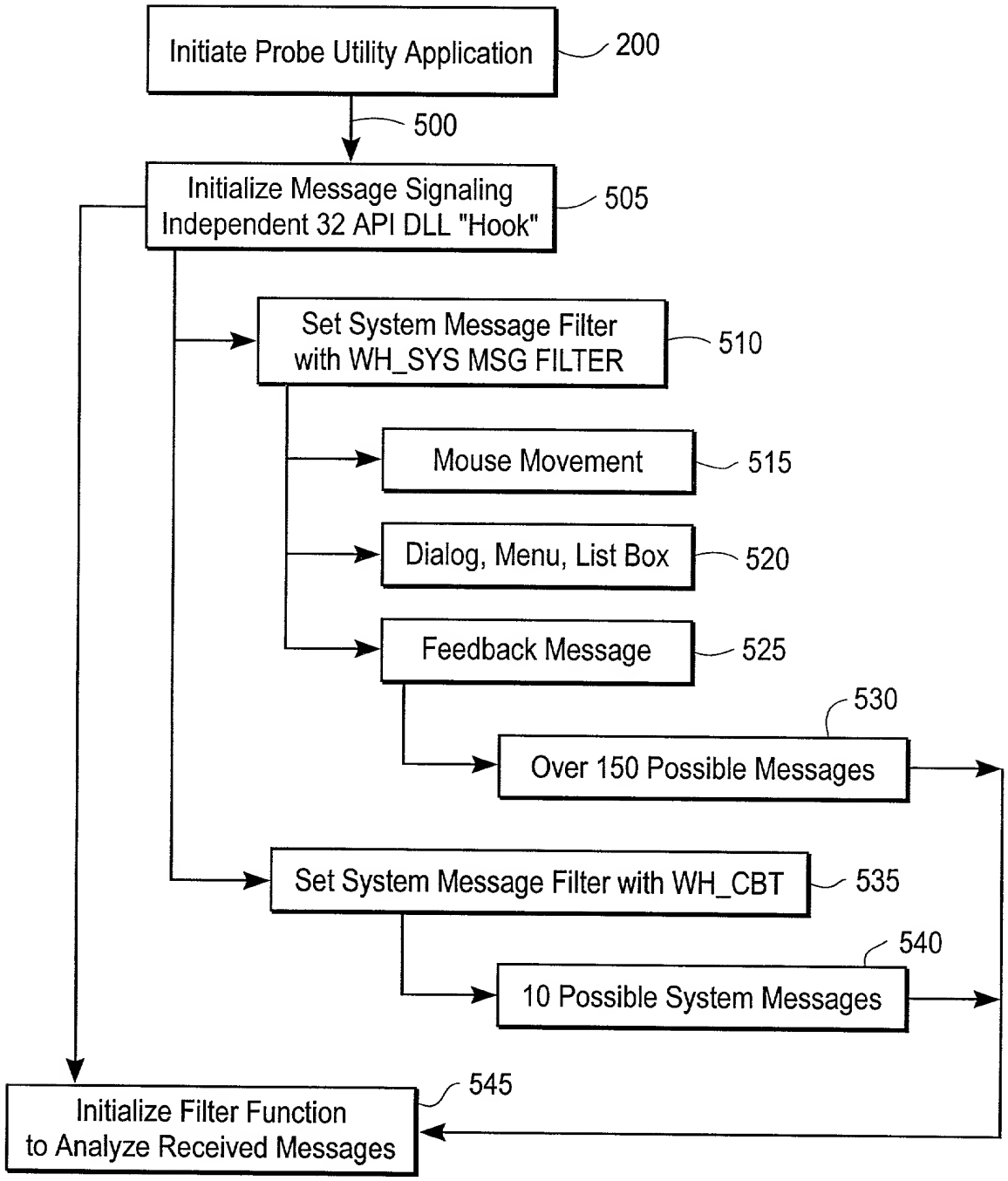

Initiate Probe Utility Application
200
500
Initialize Message Signaling Independent 32 API DLL "Hook"
505
Set System Message Filter with WH_SYS MSG FILTER
510
Mouse Movement
515
Dialog, Menu, List Box
520
Feedback Message
525
530
Over 150 Possible Messages
Set System Message Filter with WH_CBT
535
540
10 Possible System Messages
Initialize Filter Function to Analyze Received Messages
545

FIG. 5

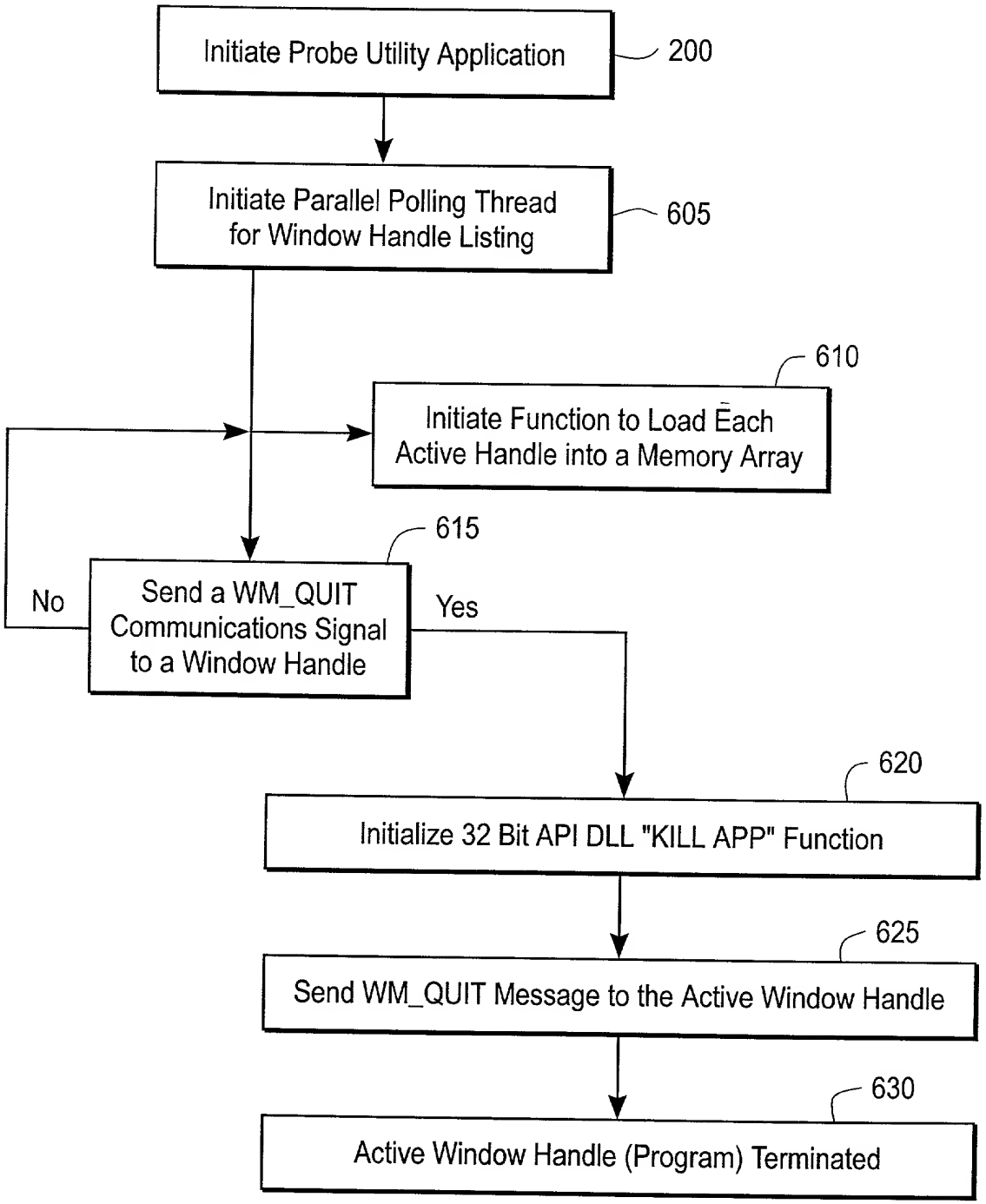

Initiate Probe Utility Application
200
Initiate Parallel Polling Thread for Window Handle Listing
605
610
Initiate Function to Load Each Active Handle into a Memory Array
615
No
Send a WM_QUIT Communications Signal to a Window Handle
Yes
620
Initialize 32 Bit API DLL "KILL APP" Function
625
Send WM_QUIT Message to the Active Window Handle
630
Active Window Handle (Program) Terminated

FIG. 6

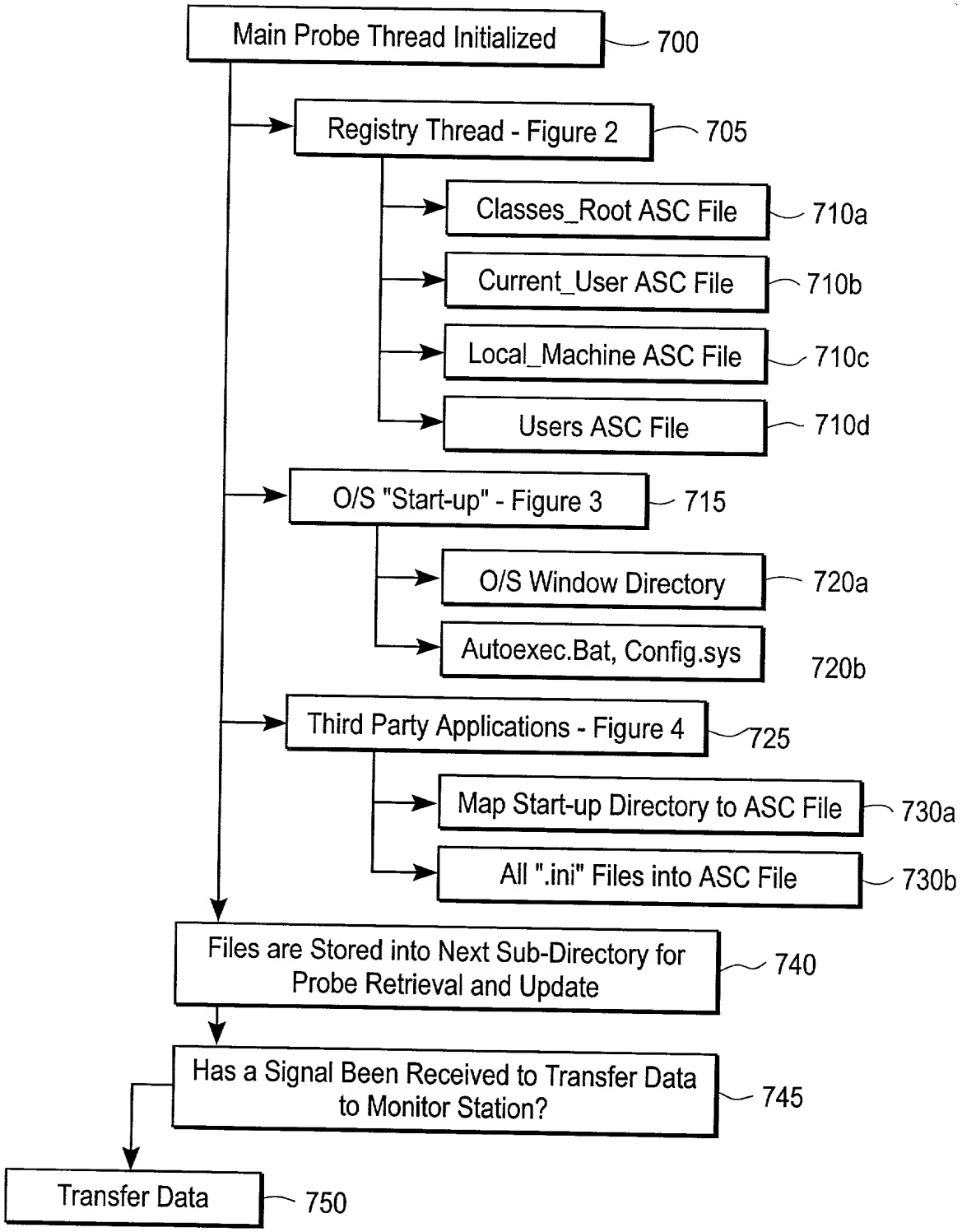

Main Probe Thread Initialized
700
Registry Thread - Figure 2
705
Classes_Root ASC File
710a
Current_User ASC File
710b
Local_Machine ASC File
710c
Users ASC File
710d
O/S "Start-up" - Figure 3
715
O/S Window Directory
720a
Autoexec.Bat, Config.sys
720b
Third Party Applications - Figure 4
725
Map Start-up Directory to ASC File
730a
All ".ini" Files into ASC File
730b
Files are Stored into Next Sub-Directory for Probe Retrieval and Update
740
Has a Signal Been Received to Transfer Data to Monitor Station?
745
Transfer Data
750

FIG. 7

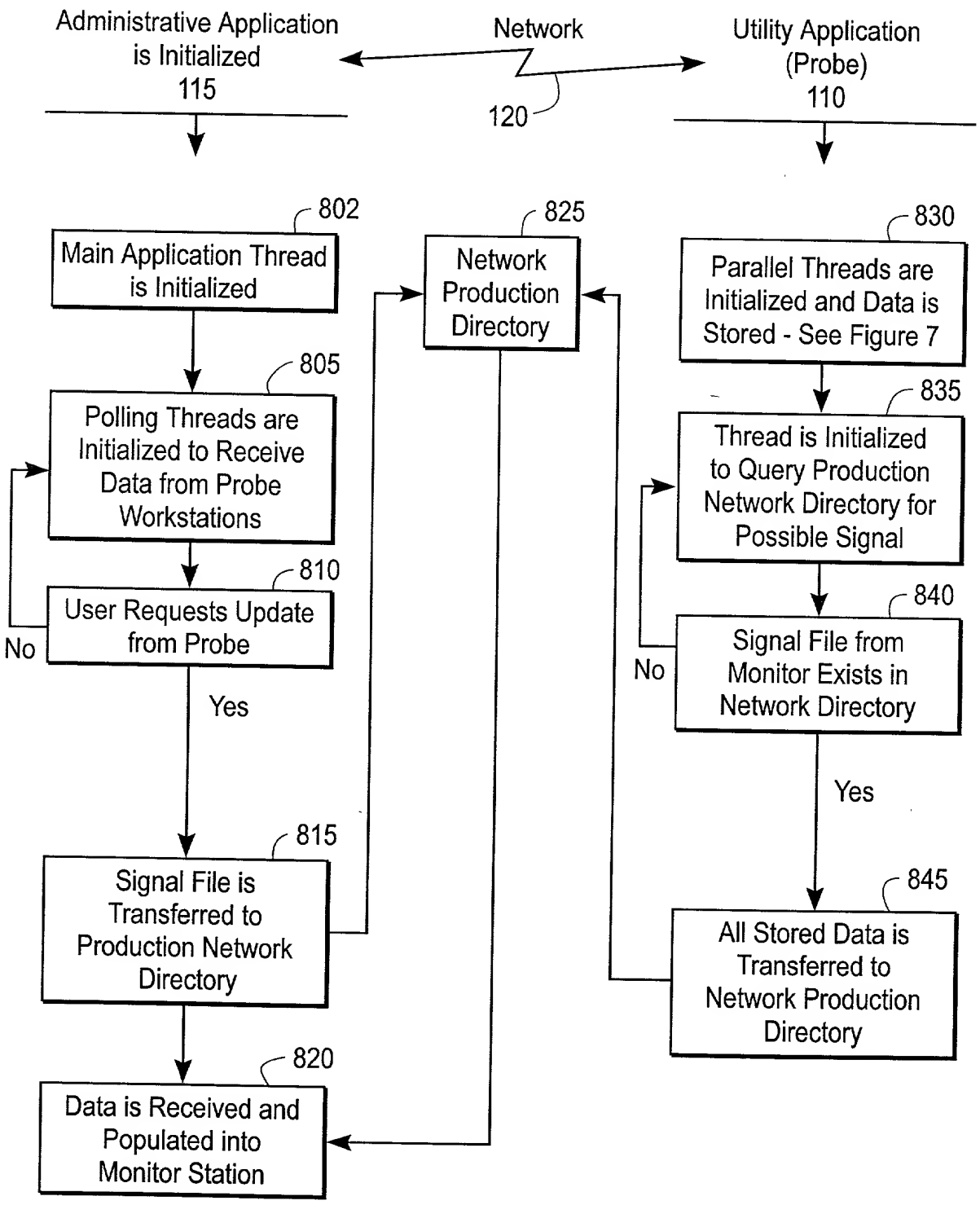

Administrative Application is Initialized 115
Network
120
Utility Application (Probe) 110
802
Main Application Thread is Initialized
805
Polling Threads are Initialized to Receive Data from Probe Workstations
810
User Requests Update from Probe
No
Yes
815
Signal File is Transferred to Production Network Directory
820
Data is Received and Populated into Monitor Station
825
Network Production Directory
830
Parallel Threads are Initialized and Data is Stored - See Figure 7
835
Thread is Initialized to Query Production Network Directory for Possible Signal
840
Signal File from Monitor Exists in Network Directory
No
Yes
845
All Stored Data is Transferred to Network Production Directory

FIG. 8

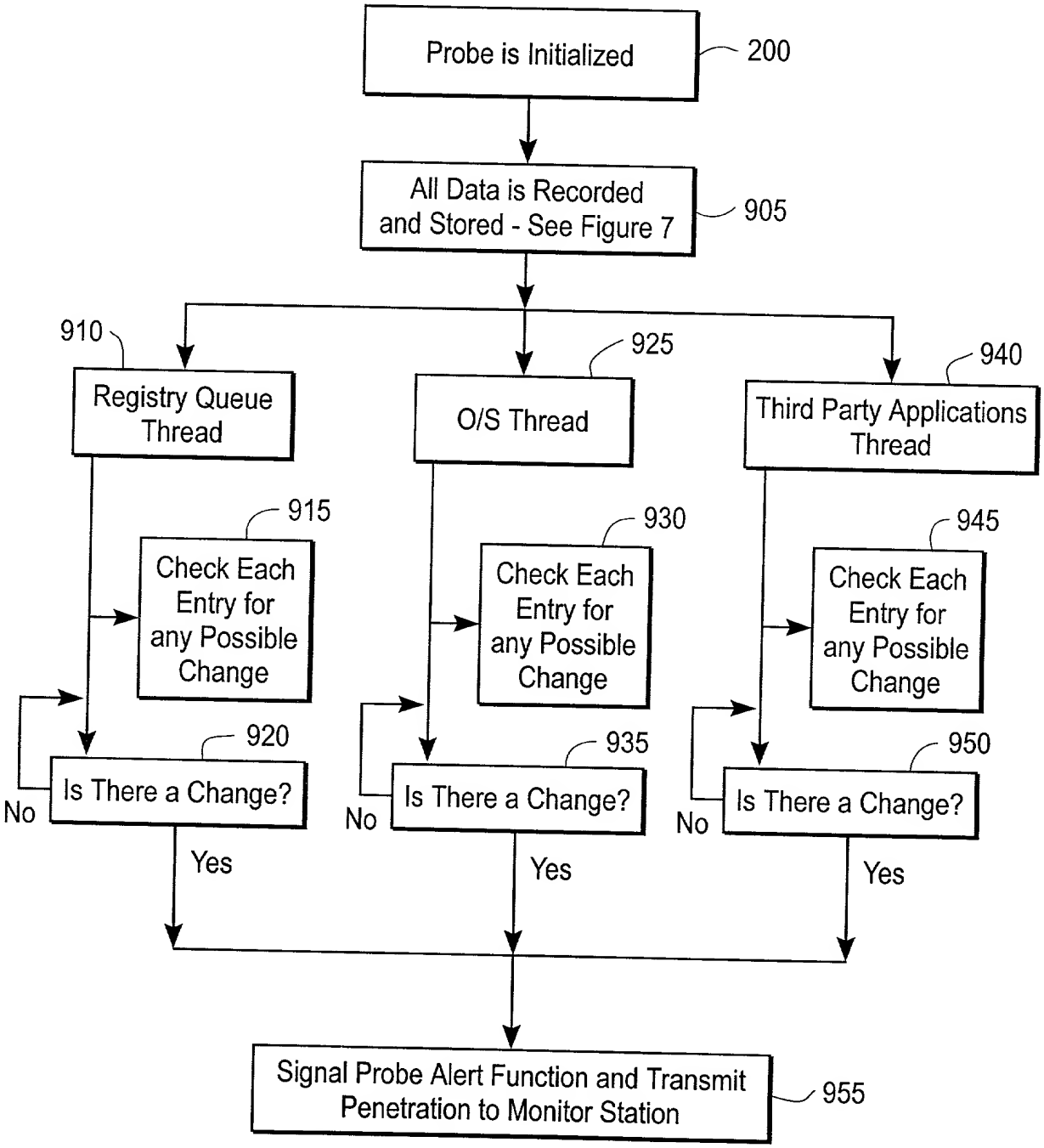

Probe is Initialized
200
All Data is Recorded and Stored - See Figure 7
905
910
Registry Queue Thread
925
O/S Thread
940
Third Party Applications Thread
915
Check Each Entry for any Possible Change
930
Check Each Entry for any Possible Change
945
Check Each Entry for any Possible Change
920
Is There a Change?
No
Yes
935
Is There a Change?
No
Yes
950
Is There a Change?
No
Yes
Signal Probe Alert Function and Transmit Penetration to Monitor Station
955

FIG. 9

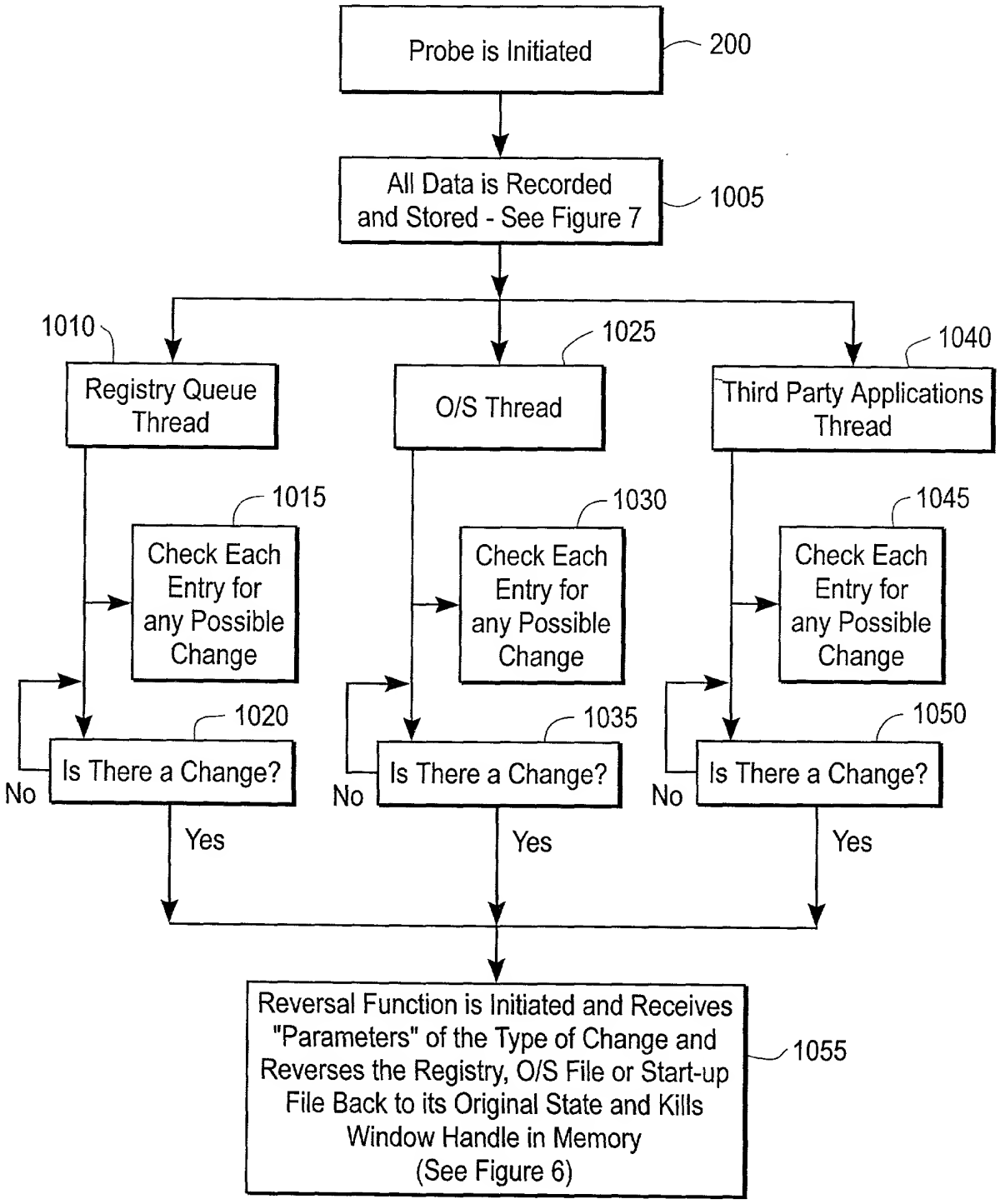
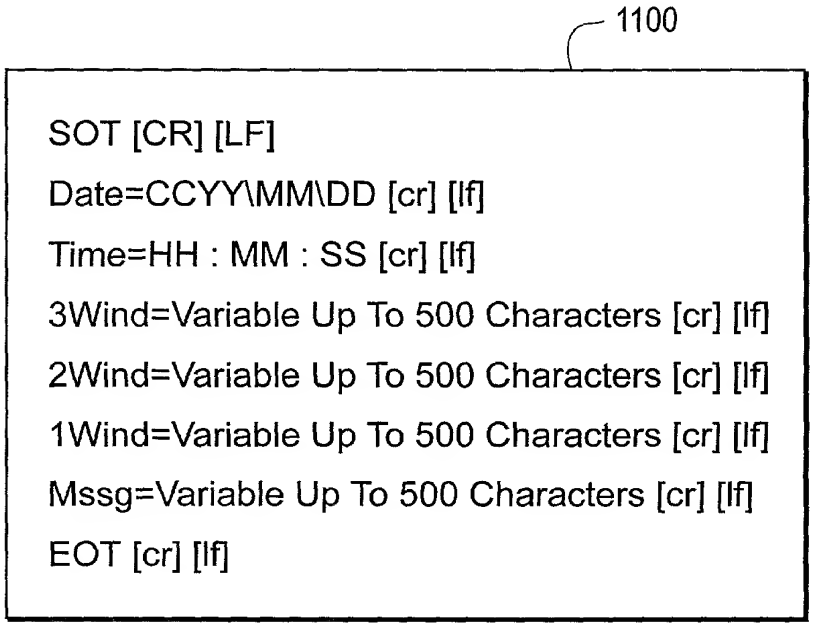


FIG. 10

Doc 1 of 1 Doc 2 of 2



Structured Signal File Block Diagram

FIG. 11

Express Mail Label No. EV 272 054 659

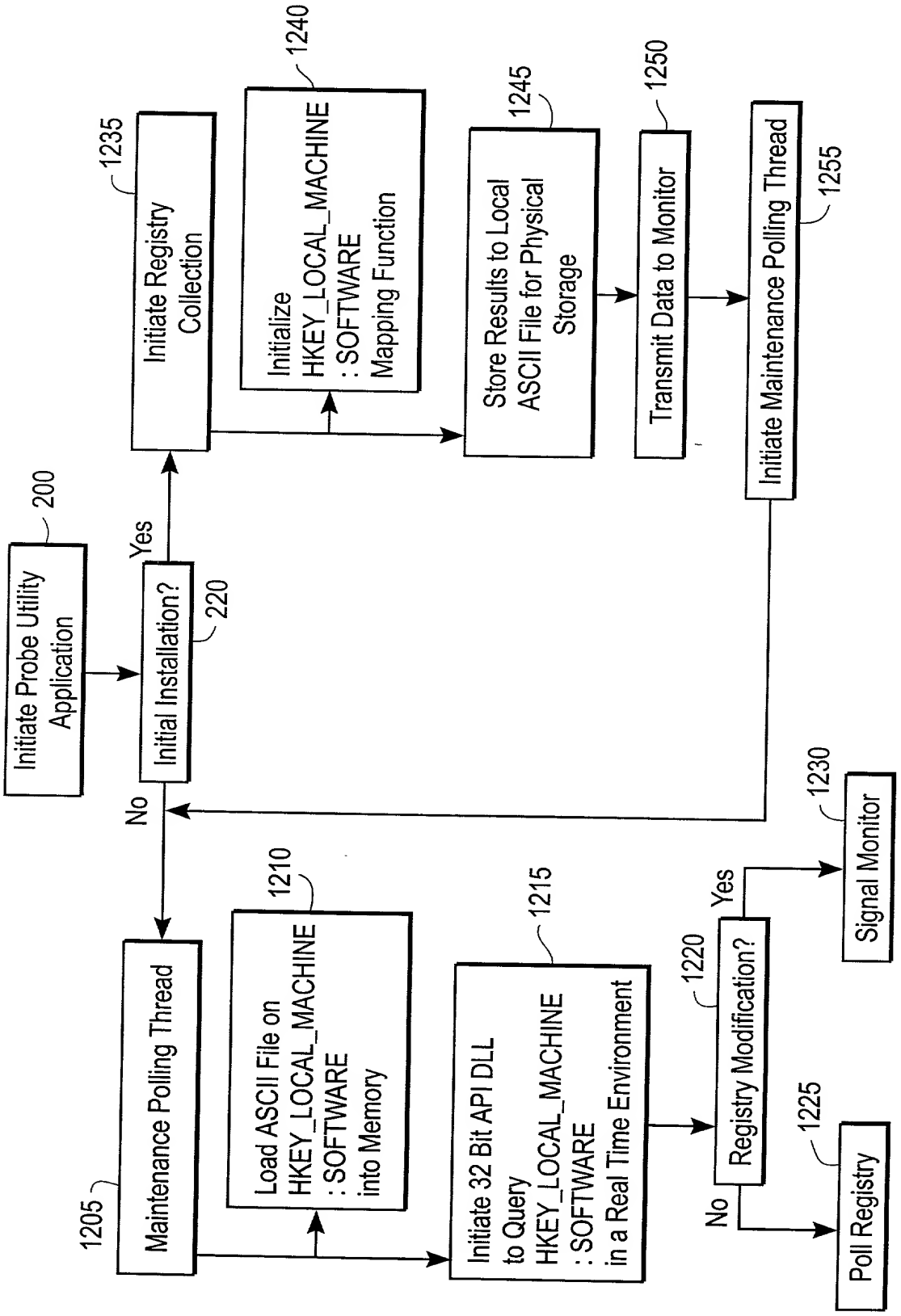

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Registry Collection
1235
Initialize HKEY_LOCAL_MACHINE : SOFTWARE Mapping Function
1240
Store Results to Local ASCII File for Physical Storage
1245
Transmit Data to Monitor
1250
Initiate Maintenance Polling Thread
1255
Maintenance Polling Thread
1205
Load ASCII File on HKEY_LOCAL_MACHINE : SOFTWARE into Memory
1210
Initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE : SOFTWARE in a Real Time Environment
1215
Registry Modification?
1220
Yes
No
Signal Monitor
1230
Poll Registry
1225

FIG. 12

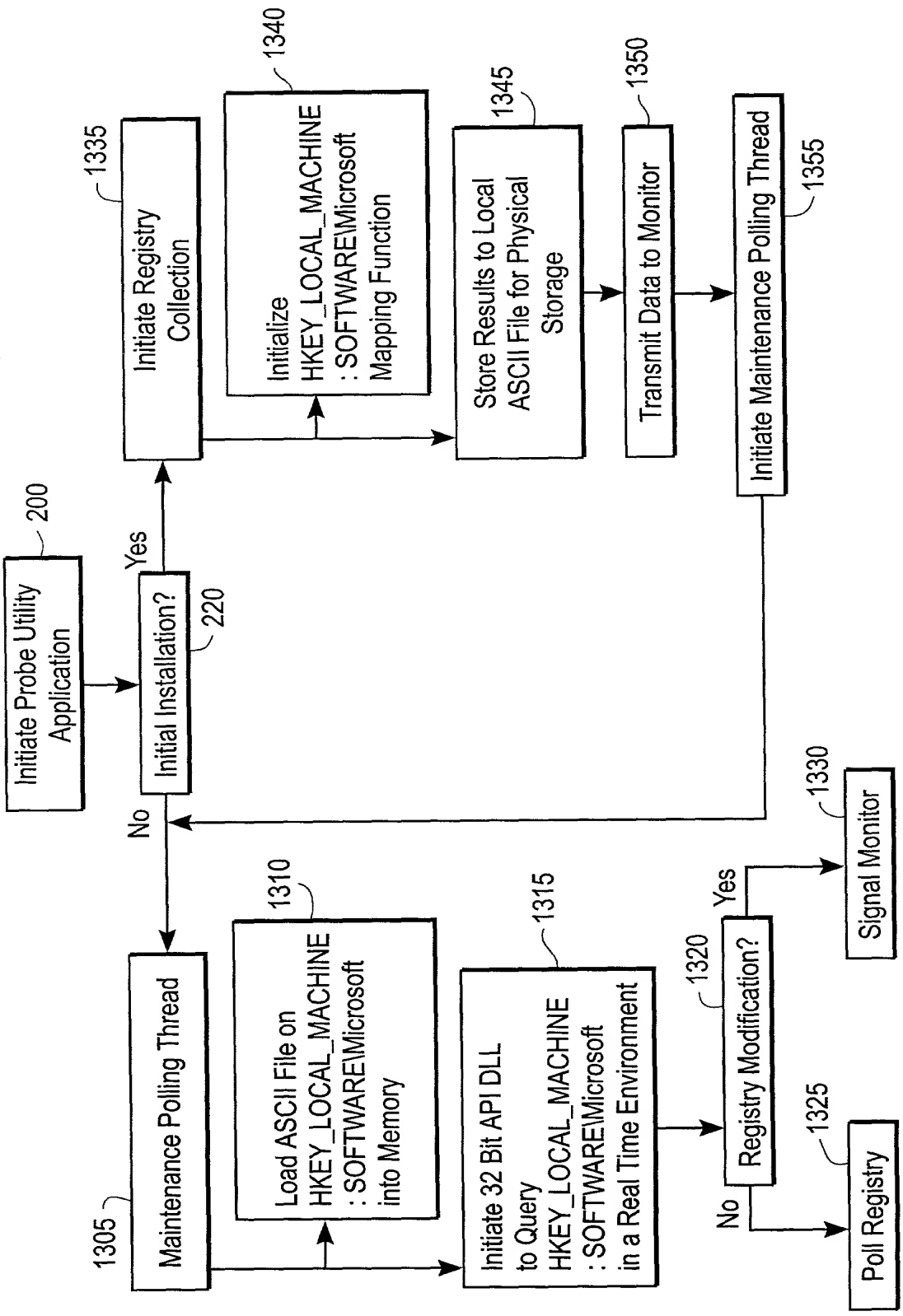

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Registry Collection
1335
Initialize HKEY_LOCAL_MACHINE : SOFTWARE\Microsoft Mapping Function
1340
Store Results to Local ASCII File for Physical Storage
1345
Transmit Data to Monitor
1350
Initiate Maintenance Polling Thread
1355
Maintenance Polling Thread
1305
Load ASCII File on HKEY_LOCAL_MACHINE : SOFTWARE\Microsoft into Memory
1310
Initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE : SOFTWARE\Microsoft in a Real Time Environment
1315
Registry Modification?
1320
Yes
No
Signal Monitor
1330
Poll Registry
1325

FIG. 13

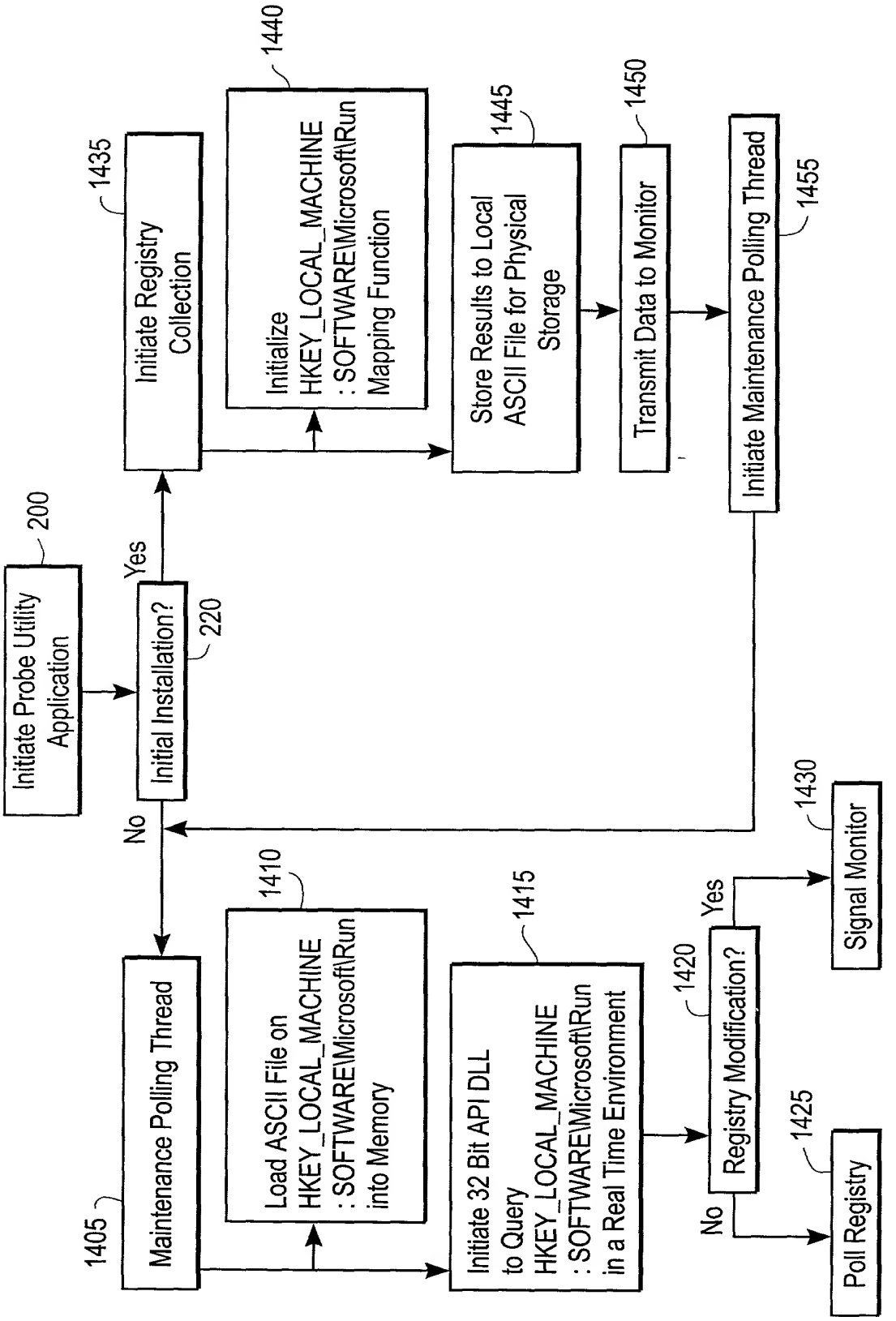

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Registry Collection
1435
Initialize HKEY_LOCAL_MACHINE : SOFTWARE\Microsoft\Run Mapping Function
1440
Store Results to Local ASCII File for Physical Storage
1445
Transmit Data to Monitor
1450
Initiate Maintenance Polling Thread
1455
Maintenance Polling Thread
1405
Load ASCII File on HKEY_LOCAL_MACHINE : SOFTWARE\Microsoft\Run into Memory
1410
Initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE : SOFTWARE\Microsoft\Run in a Real Time Environment
1415
Registry Modification?
1420
Yes
No
Signal Monitor
1430
Poll Registry
1425

FIG. 14

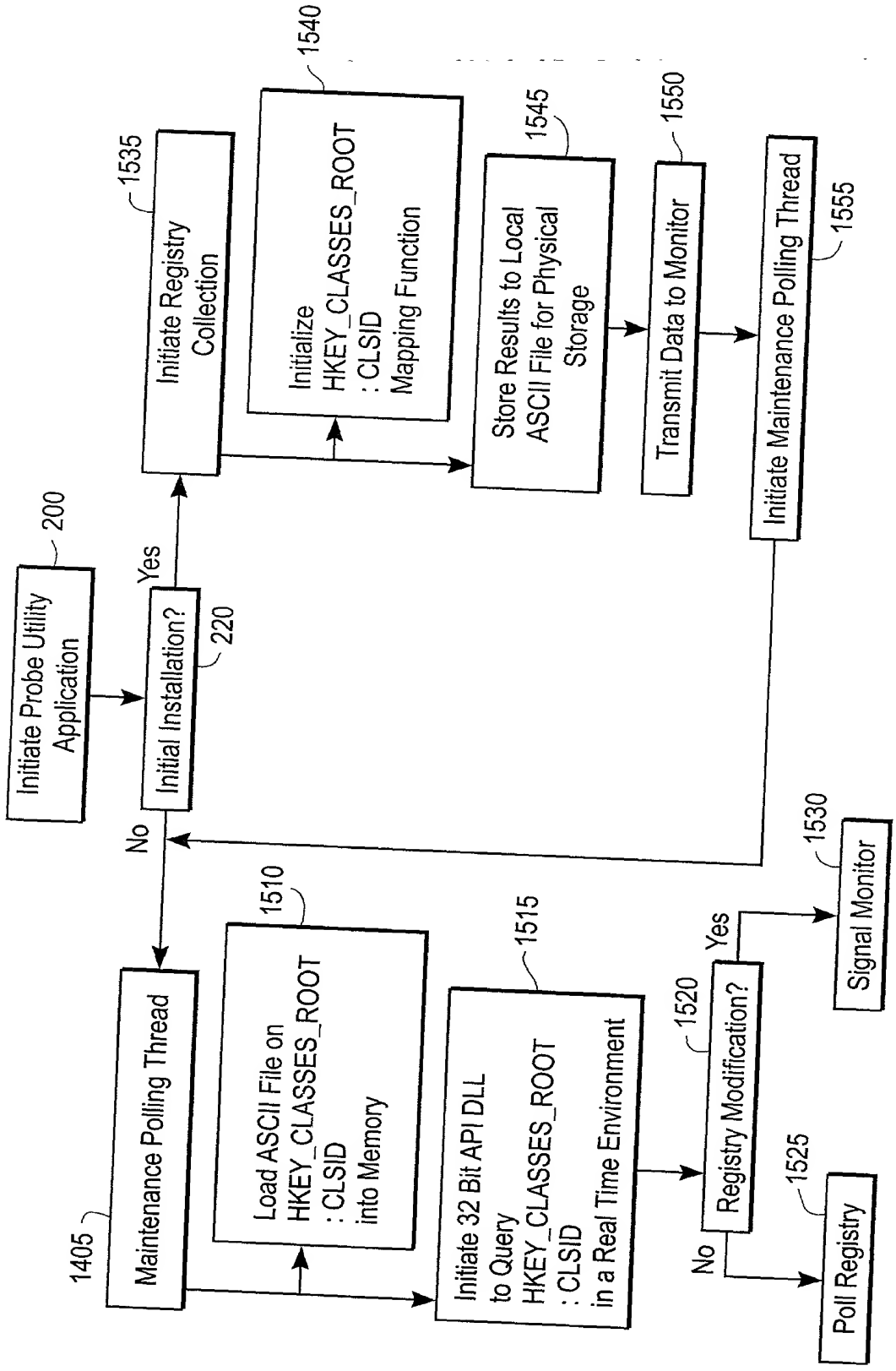

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Registry Collection
1535
Initialize HKEY_CLASSES_ROOT : CLSID Mapping Function
1540
Store Results to Local ASCII File for Physical Storage
1545
Transmit Data to Monitor
1550
Initiate Maintenance Polling Thread
1555
Maintenance Polling Thread
1405
Load ASCII File on HKEY_CLASSES_ROOT : CLSID into Memory
1510
Initiate 32 Bit API DLL to Query HKEY_CLASSES_ROOT : CLSID in a Real Time Environment
1515
Registry Modification?
1520
Yes
No
Signal Monitor
1530
Poll Registry
1525

FIG. 15

T0230 T6820860

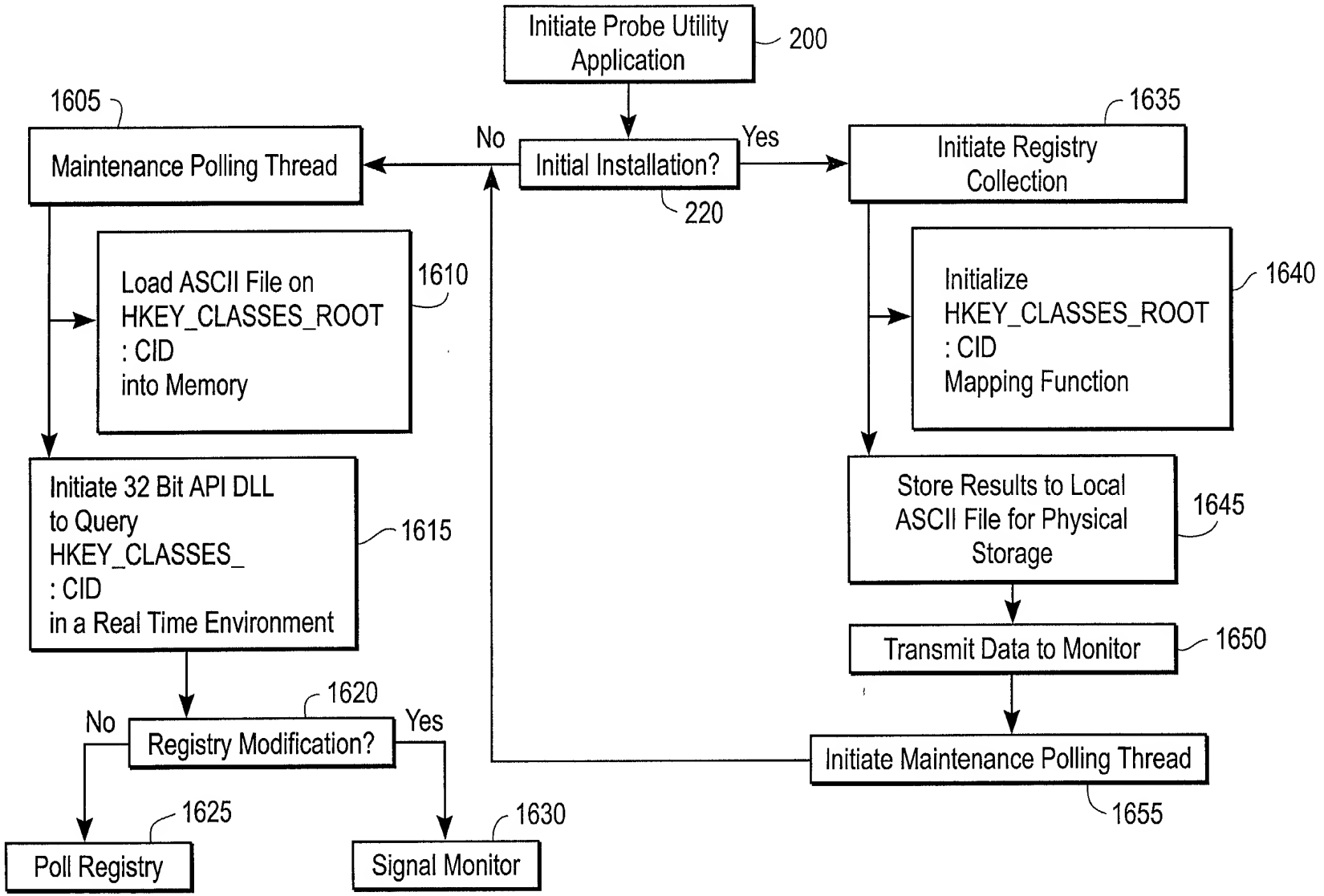


FIG. 16

Control Of Networked Computers
Inventor: Robert F. Terry
Serial No.: 09/827,891

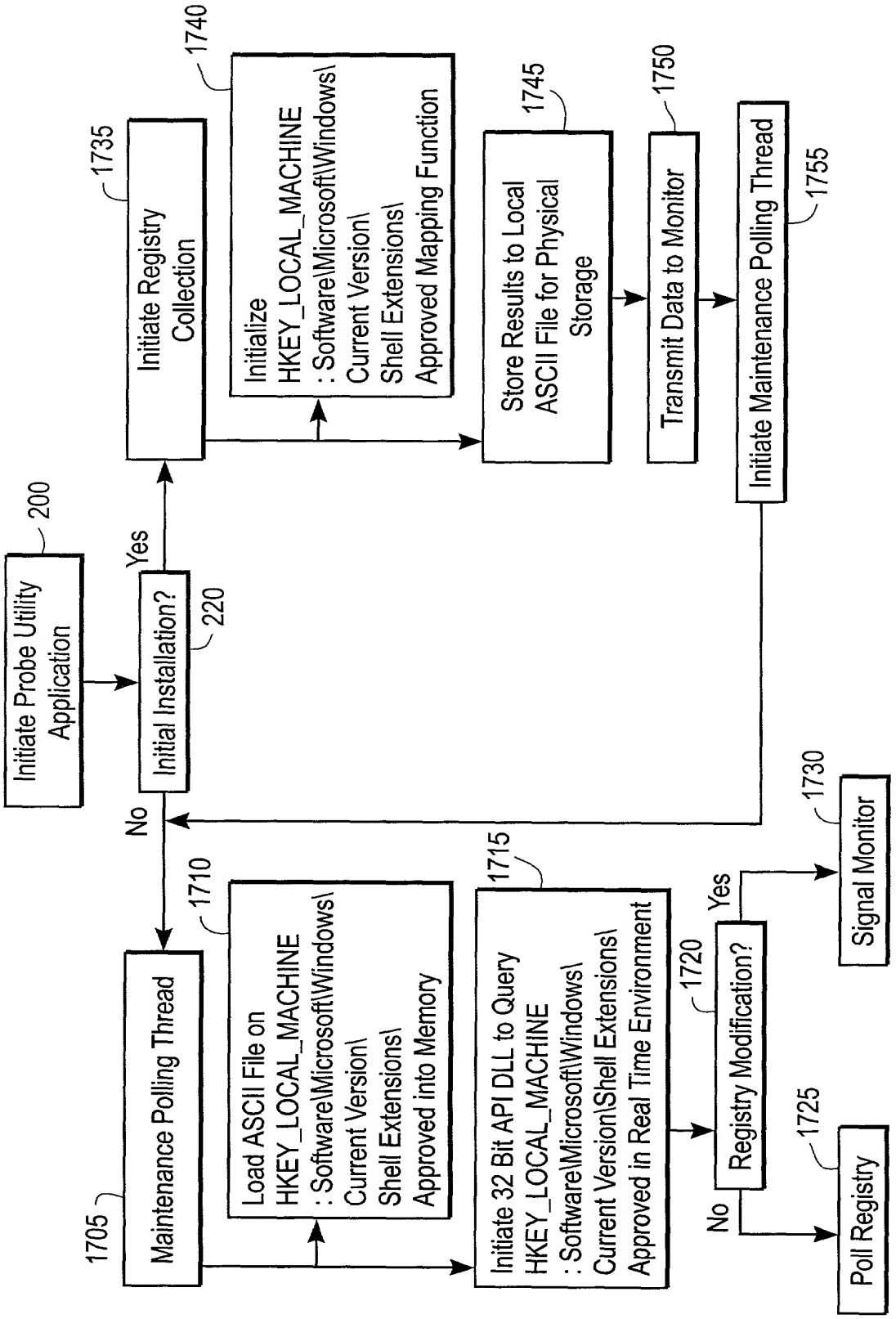

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Registry Collection
1735
Initialize HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\ Shell Extensions\ Approved Mapping Function
1740
Store Results to Local ASCII File for Physical Storage
1745
Transmit Data to Monitor
1750
Initiate Maintenance Polling Thread
1755
Maintenance Polling Thread
1705
Load ASCII File on HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\ Shell Extensions\ Approved into Memory
1710
Initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\Shell Extensions\ Approved in Real Time Environment
1715
Registry Modification?
1720
Yes
No
Signal Monitor
1730
Poll Registry
1725

FIG. 17

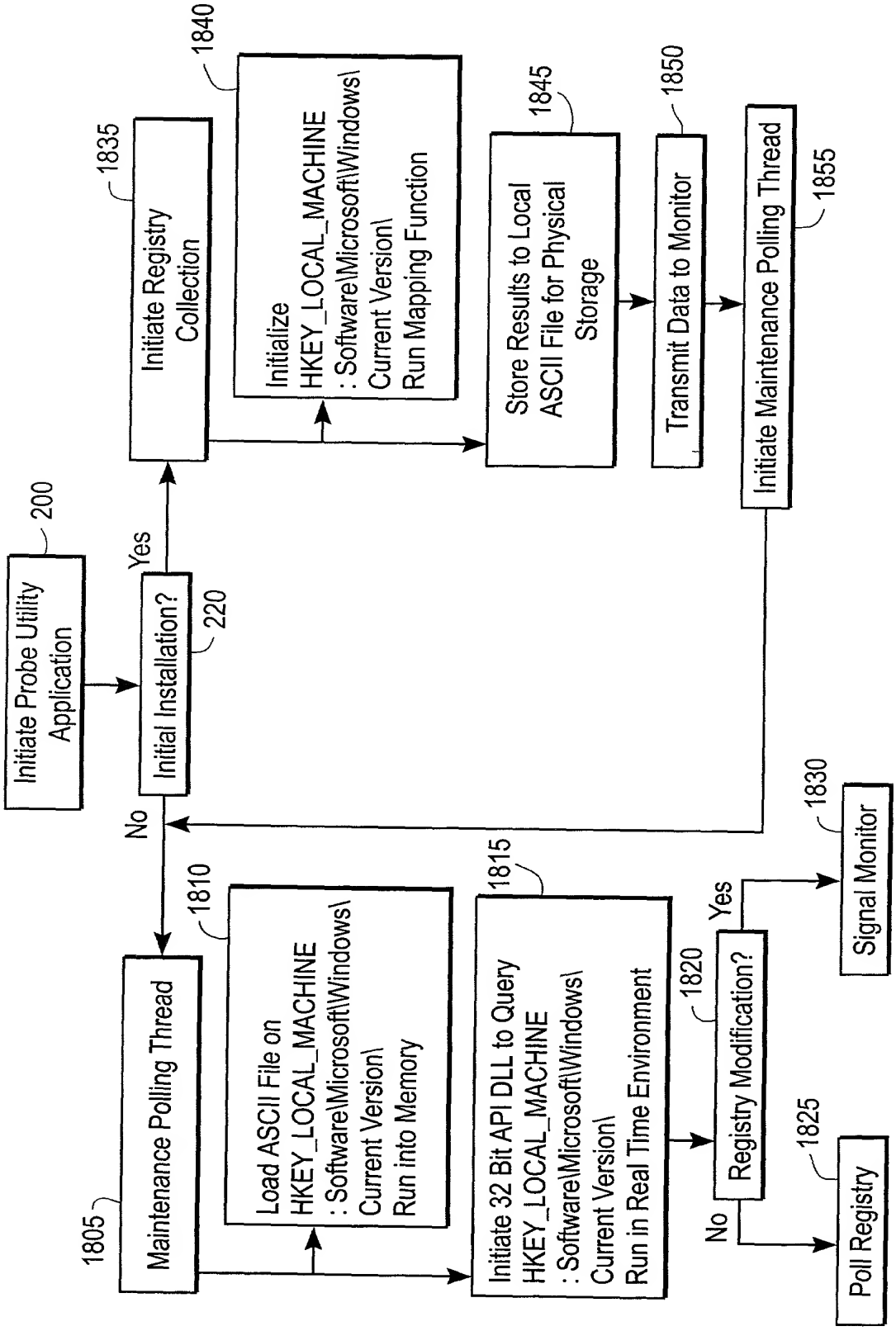

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Registry Collection
1835
Initialize HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\ Run Mapping Function
1840
Store Results to Local ASCII File for Physical Storage
1845
Transmit Data to Monitor
1850
Initiate Maintenance Polling Thread
1855
Maintenance Polling Thread
1805
Load ASCII File on HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\ Run into Memory
1810
Initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\ Run in Real Time Environment
1815
Registry Modification?
1820
Yes
No
Signal Monitor
1830
Poll Registry
1825

FIG. 18

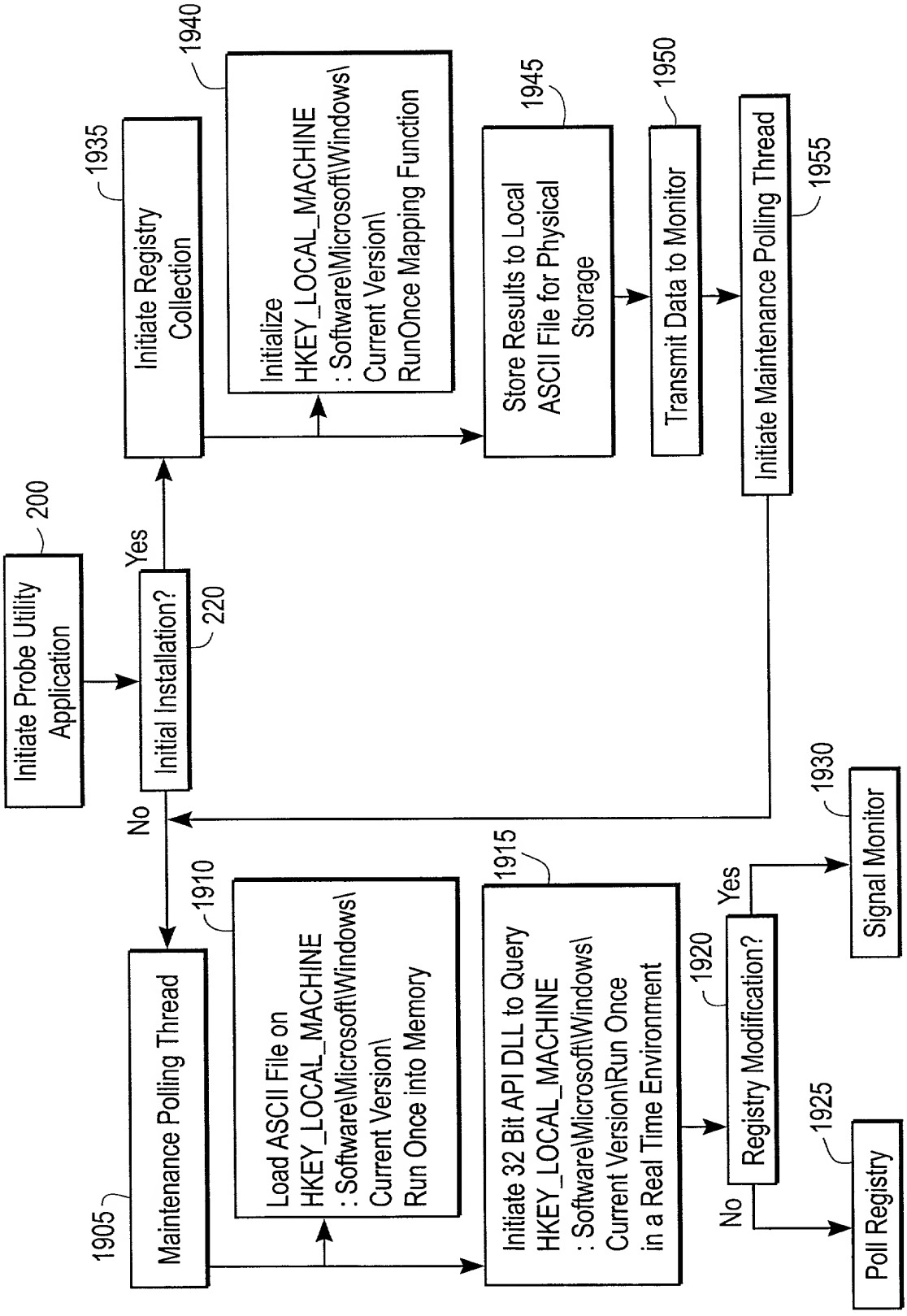

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Registry Collection
1935
Initialize HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\ RunOnce Mapping Function
1940
Store Results to Local ASCII File for Physical Storage
1945
Transmit Data to Monitor
1950
Initiate Maintenance Polling Thread
1955
Maintenance Polling Thread
1905
Load ASCII File on HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\ Run Once into Memory
1910
Initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\Run Once in a Real Time Environment
1915
Registry Modification?
1920
Yes
No
Signal Monitor
1930
Poll Registry
1925

FIG. 19

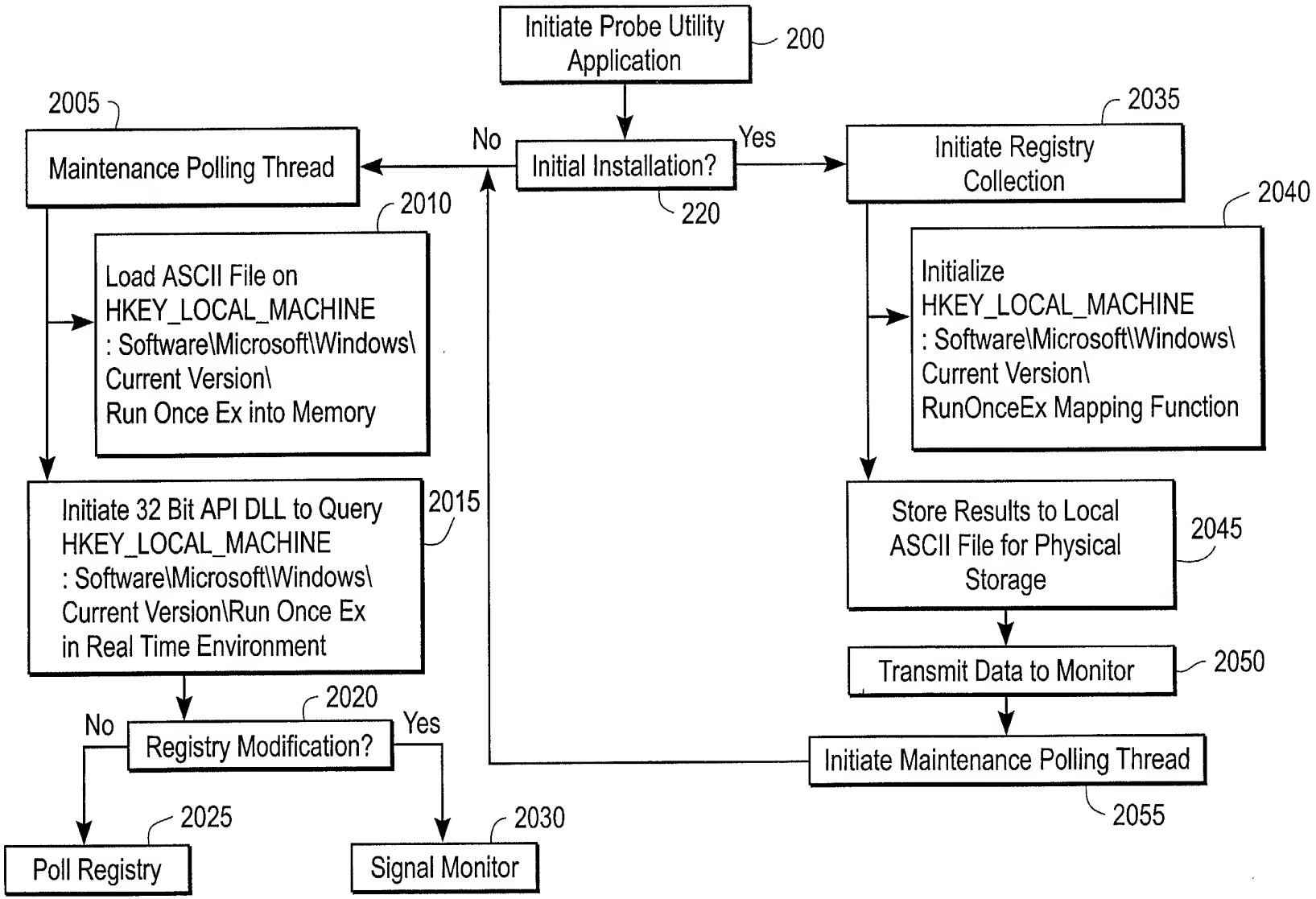

Initiate Probe Utility Application
200
Initial Installation?
220
No
Yes
2005
Maintenance Polling Thread
2010
Load ASCII File on HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\ Run Once Ex into Memory
Initiate 32 Bit API DLL to Query HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\Run Once Ex in Real Time Environment
2015
2020
Registry Modification?
No
Yes
2025
Poll Registry
2030
Signal Monitor
2035
Initiate Registry Collection
2040
Initialize HKEY_LOCAL_MACHINE : Software\Microsoft\Windows\ Current Version\ RunOnceEx Mapping Function
Store Results to Local ASCII File for Physical Storage
2045
Transmit Data to Monitor
2050
Initiate Maintenance Polling Thread
2055

FIG. 20

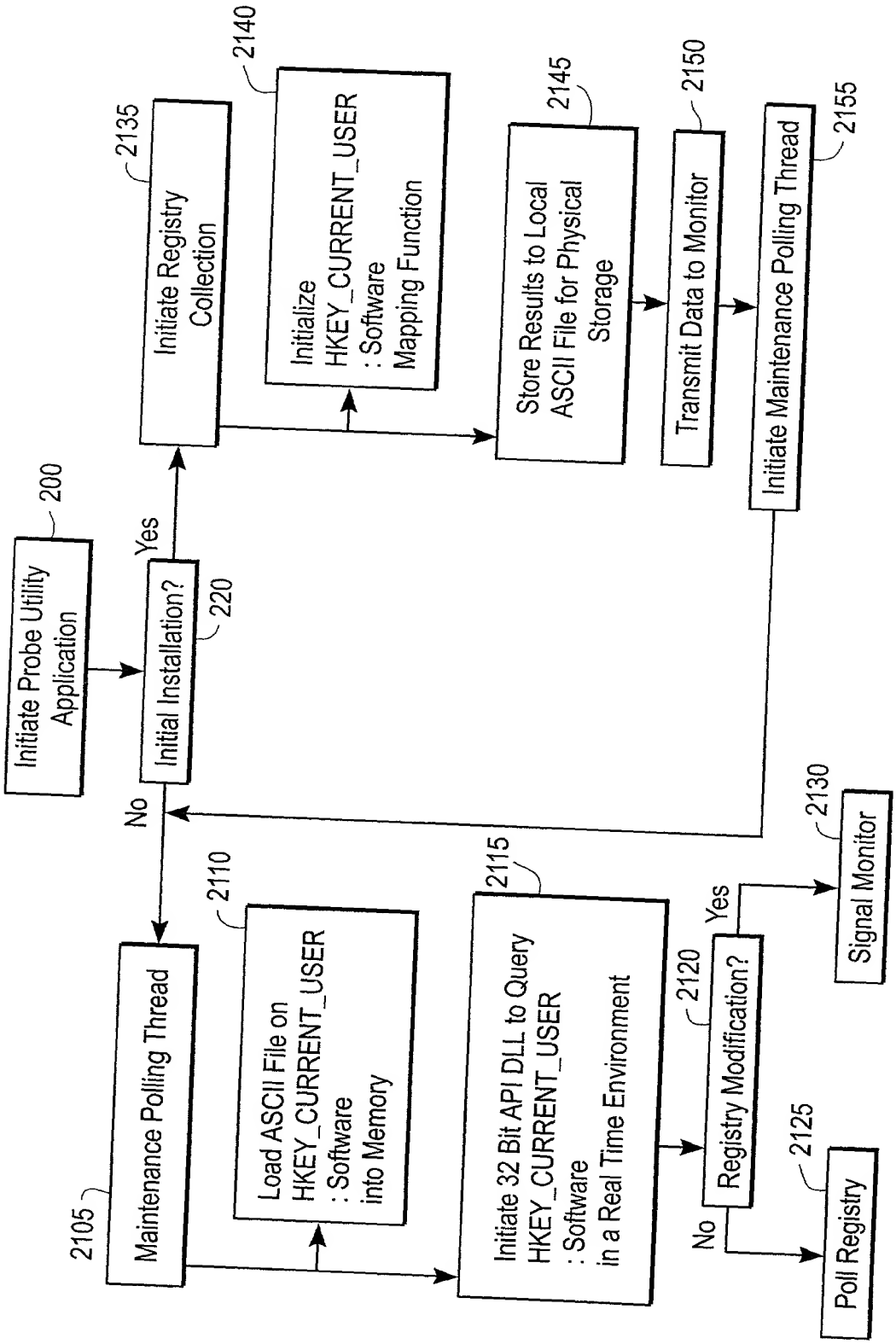

Initiate Probe Utility Application
200
Initial Installation?
220
Yes
No
Initiate Registry Collection
2135
Initialize HKEY_CURRENT_USER : Software Mapping Function
2140
Store Results to Local ASCII File for Physical Storage
2145
Transmit Data to Monitor
2150
Initiate Maintenance Polling Thread
2155
Maintenance Polling Thread
2105
Load ASCII File on HKEY_CURRENT_USER : Software into Memory
2110
Initiate 32 Bit API DLL to Query HKEY_CURRENT_USER : Software in a Real Time Environment
2115
Registry Modification?
2120
Yes
No
Signal Monitor
2130
Poll Registry
2125

FIG. 21

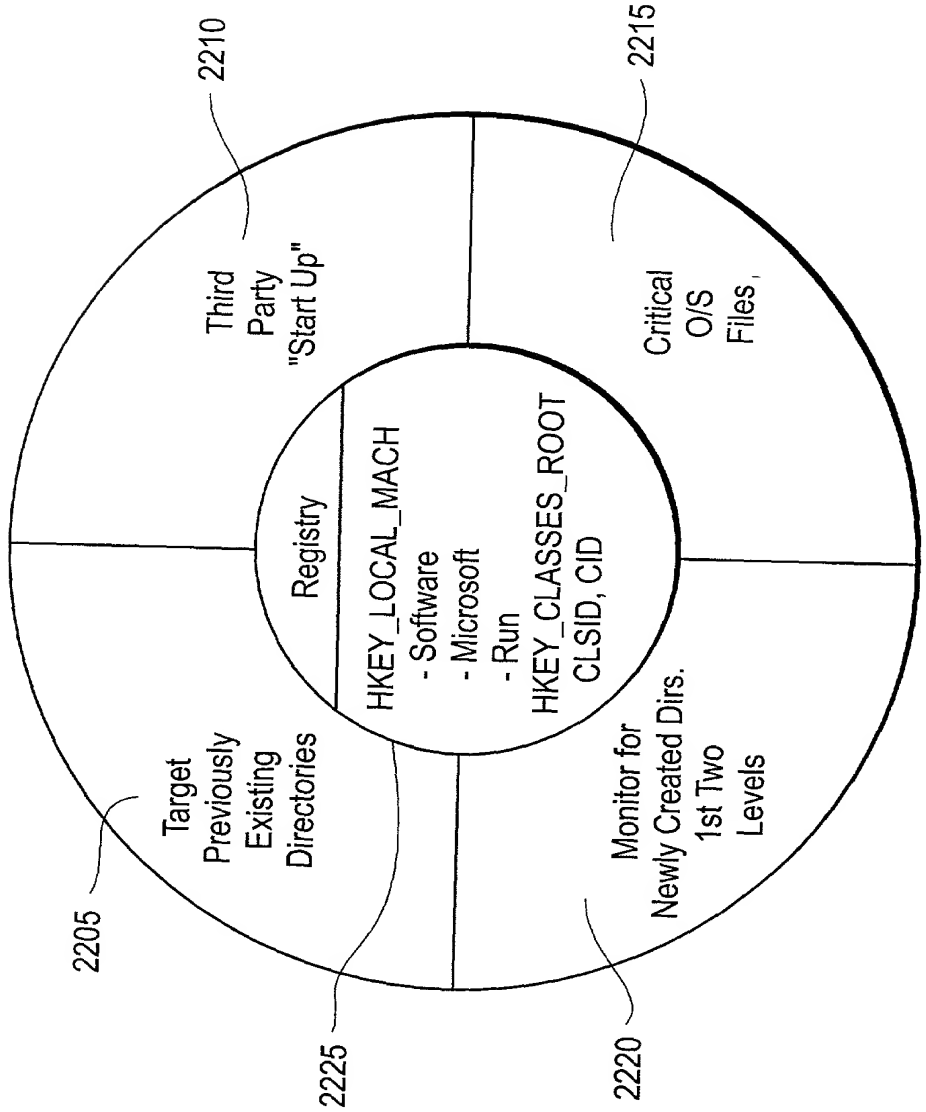

GTI "Defense Umbrela"
2210
Third Party "Start Up"
2215
Critical O/S Files,
Registry
HKEY_LOCAL_MACH
- Software
- Microsoft
- Run
HKEY_CLASSES_ROOT
CLSID, CID
2205
Target Previously Existing Directories
2225
2220
Monitor for Newly Created Dirs. 1st Two Levels
"Guarded State" of the Complete PC

FIG. 22

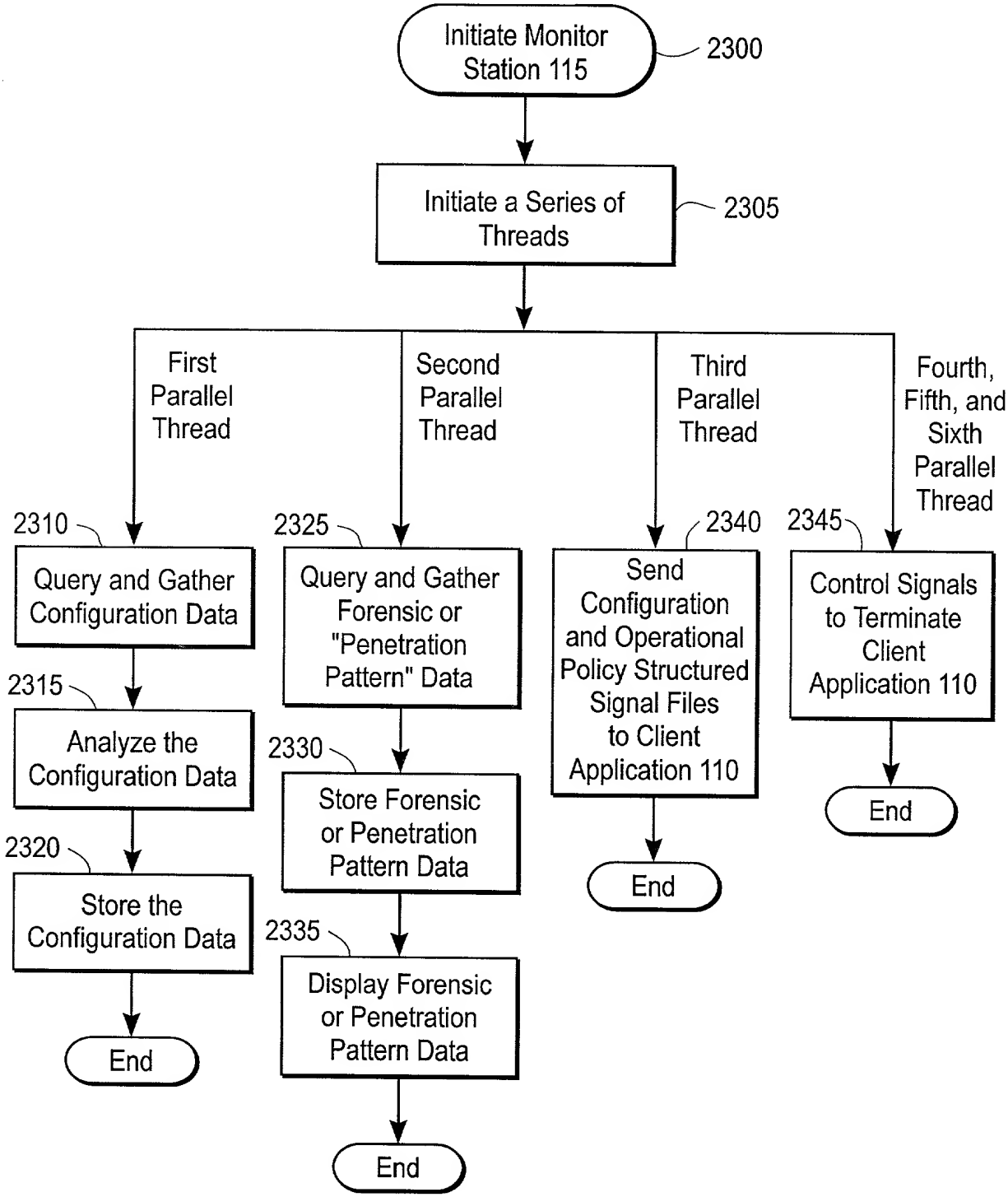

Initiate Monitor Station 115
2300
Initiate a Series of Threads
2305
First Parallel Thread
Second Parallel Thread
Third Parallel Thread
Fourth, Fifth, and Sixth Parallel Thread
2310
Query and Gather Configuration Data
2315
Analyze the Configuration Data
2320
Store the Configuration Data
End
2325
Query and Gather Forensic or "Penetration Pattern" Data
2330
Store Forensic or Penetration Pattern Data
2335
Display Forensic or Penetration Pattern Data
End
2340
Send Configuration and Operational Policy Structured Signal Files to Client Application 110
End
2345
Control Signals to Terminate Client Application 110
End

FIG. 23

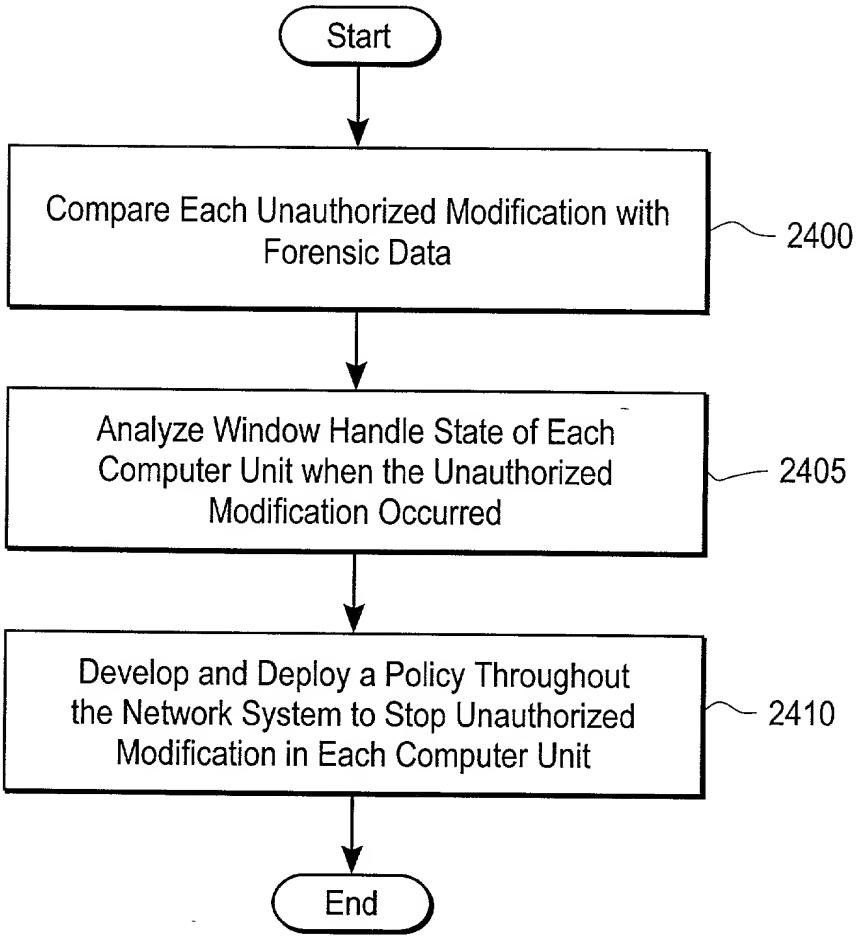

Start
Compare Each Unauthorized Modification with Forensic Data
2400
Analyze Window Handle State of Each Computer Unit when the Unauthorized Modification Occurred
2405
Develop and Deploy a Policy Throughout the Network System to Stop Unauthorized Modification in Each Computer Unit
2410
End

FIG. 24